# Measuring Accumulated Revelations of Private Information by Multiple Media

Komei Kamiyama, Tran Hong Ngoc, Isao Echizen, Hiroshi Yoshiura

# Measuring Accumulated Revelations of Private Information by Multiple Media

Komei Kamiyama [1], Tran Hong Ngoc [2], Isao Echizen [3], and Hiroshi Yoshiura [4]

[1] Department of Human Communication, The University of Electro-Communications, 1-5-1 Chofugaoka Chofu, Tokyo, 182-8585 Japan.
[2] Faculty of Information Technology, University of Science, VNU- HCMC227 Nguyen Van Cu, Dist. 5, Ho Chi Minh City, Vietnam.
[3] Digital Content and Media Sciences Research Division, National Institute of Informatics 2-1-2 Hitotsubashi, Chiyodaku, Tokyo, 101-8430 Japan.
[4] Department of Informatics, The University of Electro-Communications, 1-5-1 Chofugaoka Chofu, Tokyo, 182-8585 Japan.
kamiyama@edu.hc.uec.ac.jp, yoshiura@hc.uec.ac.jp

**Abstract.** A metric has been developed for measuring privacy degradation when various types of media reveal private information about a person. The metric, which is based on joint entropy, quantifies accumulated revelations of information about various personal attributes. Application of this metric to entries posted on a social networking service and to leaks from a company database containing personal information showed that it is effective; that is, it can quantify accumulated revelations of information about multiple attributes and can cope with cases in which the attributes affect each other.

**Keywords:** Privacy, Privacy metric, Social Networking Service

## 1 Introduction

Private information about various attributes of people is acquired, stored, and made available by various types of media in Web2.0 and in ubiquitous networks, and it can be revealed in a number of ways. For instance, friends may disclose private information on social network services (SNSs), third parties may illegally access information residing in databases belonging to public organizations and enterprises, computer viruses may obtain private information residing on PCs and send it over the network, and ubiquitous networks may automatically obtain and reveal personal location information.

Such revelations of private information can lead to serious problems. Leaks of private information may result in a person receiving annoying e-mails, being stalked, or even being fired from their job. Moreover, even if there is no actual damage, people might feel anxious about using network services upon hearing of the danger.

Internet service providers (ISPs) can be the source of revealed private information. The revelations may be unintentional or the result of malicious behaviours by an employees. ISPs must therefore take privacy protection seriously while still ensuring system usability. Privacy metrics are therefore important for analysing the trade-off between privacy protection and system usability. Users also reveal their private information carelessly or voluntarily without being able to predict consequence of the disclosure. Thus, privacy metrics are important to detect such revelation by users

Metrics for quantifying privacy have been proposed for privacy-preserving data mining, location privacy, and e-mail. Most of these metrics are application dependent, but metrics based on k-anonymity and entropy can generally be used. However, such metrics cannot quantify accumulated revelations of information about different attributes. In particular, metrics based on k-anonymity and entropy cannot cope with cases in which multiple attributes are not mutually independent, and, in the real world, such attributes are not usually independent. Assume, for example, that a person posted an entry on his/her SNS page saying "I am struggling everyday to save lives of people" and that he/she is known to graduate from The University of Tokyo from information illegally obtained from a company database. The combination of these two information revelations enables the estimate of his/her occupation (i.e. medical doctor) and his/her educational record (i.e. M.D. conferred by The University of Tokyo). Metrics based on k-anonymity and entropy cannot measure the accumulation of these information revelations.

We have developed a metric for measuring multiple revelations of information by using joint entropy. Section 2 describes the revelation of information about multiple attributes. Section 3 describes related work. Section 4 describes our privacy model. Section 5 describes our metric, and Section 6 describes its application to SNS entries and a company database and evaluates its performance. Section 7 concludes the paper with a brief summary of the key points.

## 2 Revelations by various types of media

Suppose that a person posts the following entry on an SNS.

*Entry 1:* I attend a *technical university in Tokyo*.

From this entry, a reader could identify a number of universities that the writer might be attending. The next day, the writer posts another entry.

*Entry 2: Next week, I plan to attend the job fair in the West-6 building*.

From entry 2, the reader learns that the writer's university has a building named "West-6". If both entries are considered together, the reader can limit the field because only two universities have buildings named "West-6", i.e. UEC (The University of elctro-communication) and Tokyo Tech (Tokyo Institute of Technology). Because the number of students at UEC and Tokyo Tech are 4165 and 4911, the probabilities of the writer attending UEC and Tokyo Tech are 4165/9076 and 4911/9076.

Now, let us suppose that the writer's hometown is in Kyoto and that this information has been leaked from a company database. Moreover, because UEC and Tokyo Tech respectively have 28 and 16 students from Kyoto, the probabilities of the writer attending one of these universities can be calculated more precisely. Numbers of students of UEC and Tokyo Tech as well as those from each prefecture are public data provided by these universities. Therefore any attacker can use these data to estimate the writer's privacy.

Furthermore, we assume that the attacker obtains the record of writer's location at every one hour in daytime of five weekdays, i.e. the attacker has 40 data items of location. If 19 location data items are those of UEC and no data items Tokyo Tech, the confidence that the writer belongs to UEC is increased.

As shown by this example, revelations of private information can have a combinatorial effect. Thus, a privacy metric for the real world should be able to quantify mutually dependent information disclosures.

## 3 Related work

Privacy can be quantified as the degree of uncertainty about which private data can be inferred. The metric developed by Agrawal and Srikant et al.[1] for protecting privacy during data mining adds a random perturbation to each attribute of the data including personal information. Privacy is quantified by evaluating how closely the original value of an attribute can be estimated. That is, if the original value can be estimated with c% confidence to lie in interval [a,b], the interval width (b-a) defines the amount of privacy at the c% confidence level. However, they did not consider the distribution of the original data. Therefore Agrawal and Aggarwal et al. improved this metric by using entropy [2].

Sweeney proposed a different approach to privacy protection during data mining: using k-anonymity [3]. If a data table satisfies k-anonymity, every record in that table is indistinguishable from at least k − 1 other records with respect to every set of quasi-identifier attributes. The possible attacks against k-anonymity include homogeneity attacks and background-knowledge attacks focused on the quasi-identifiers. These problems of k-anonymity can be solved by adding l-diversity, which requires that each equivalent class of records in k-anonymity has at least l well-represented values of the sensitive attribute [4]. In t-closeness [5], the distribution of the sensitive attribute values in each equivalent class is close to that in the whole table.

Hoh and Gruteser's [6] location privacy metric uses the expected error in the distance between a person's true location and the attacker's uncertain estimates of that location. Duckham and Kulik [7] defined the "level of privacy" as the number of different location coordinates sent by a user with a single location-based query. Gruteser and Grunwald introduced k-anonymity to location privacy [8] and used k to represent the level of privacy. Hoh et al. [9] quantified location privacy as the duration over which an attacker could track a target person. Some studies on location privacy have taken into account the relationship between location privacy and quality of service[10][11].

Claudia, D. et al.[12] and Andrei, S. et al. [13]proposed metric for E-mail by using entropy. Serjantov et al. also applied their metric to the anonymity of voting system. Ryouke , Y., and Astushi, K., et al proposed probabilistic metric quantifying the degree of personal information disclosure from blog [18].

While most of the above metrics are application dependent, metrics based on k-anonymity and entropy can generally be used to quantify privacy for any kind of media. However, they cannot cope with situations like those described in section 2 because they cannot quantify the accumulated revelations of private information about different attributes and they cannot cope with cases in which the multiple attributes are not independent.

## 4 Our model of privacy

The anonymity metric based on entropy, which was proposed independently by Claudia, D. et al.[12] and Andrei, S. et al. [13], focuses on one particular action. An anonymity set is defined that contains the people who might take the action. For each person, the probability of taking the action is given. The degree of anonymity is

defined as the value of the entropy calculated from the anonymity set and the probabilities.

Inspired by this anonymity metric, we propose a privacy metric. We use the symmetry relation between anonymity and privacy [14]. We focus on one particular person, i.e. the subject of our privacy metric. We first consider one attribute of the subject and define a privacy set containing the potential attribute values. The probability that the attribute takes each value is given. The degree of privacy is defined as the value of entropy calculated from the privacy set and the probability (Fig. 1).

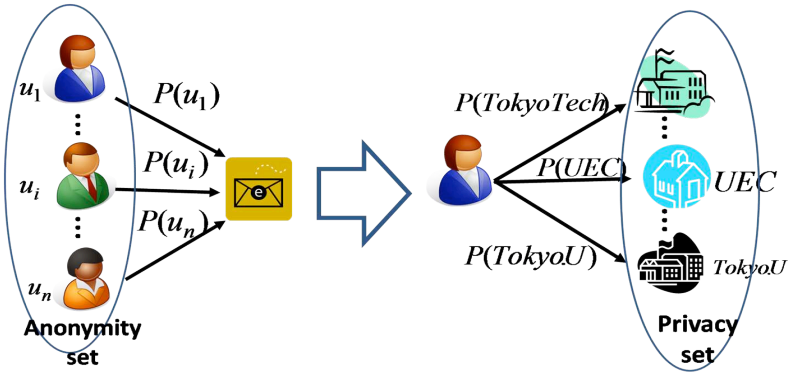


**Fig. 1. Anonymity and privacy**

Next, we consider multiple attributes of the subject and the combination of the privacy sets for the attributes (Fig. 2, left). Finally, we consider the privacy in the case where the attributes affect each other (Fig. 2, right). As described in Section 2, disclosing that the subject's hometown is Kyoto increases the probability that the subject attends UEC. The increase in this probability leads to a decrease in the probability that the subject majors in economics and increases the probability that the subject majors in computer science. We use joint entropy to represent these relations between attributes. Thus, the revelation of private information is quantified in terms of the difference in joint entropy before and after information is disclosed.

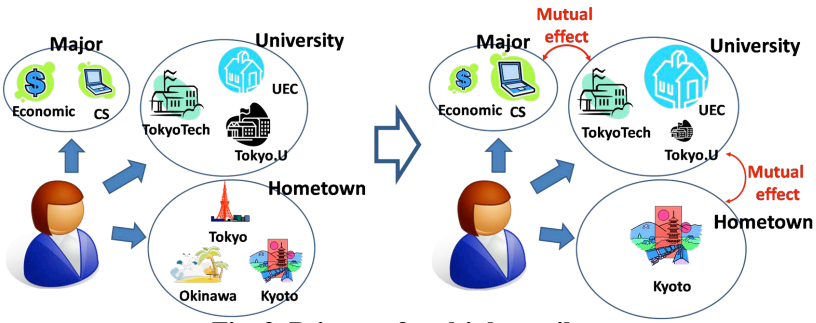


**Fig. 2. Privacy of multiple attribute**

# 5 Metric of privacy revelation

## 5.1 Definition

We first model the problem and define the terms.

Attributes and attribute values

We assume that the person of interest (*the subject of our privacy metric*) has $m$ attributes. We define $\chi^{(k)}$ to be the set of all potential attribute values of $k \in \{1,\ldots,m\}$. Moreover, $\chi^{(1)},\chi^{(2)},\ldots,\chi^{(m)}$ have mutually exclusive attribute values: $\chi^{(1)} \cap \chi^{(2)} \cap \ldots \cap \chi^{(m)} = \phi$.

**Table1. Examples of attributes and their values**

| Attributes | Attribute values | Notation |
|---|---|---|
| university | UEC, Tokyo Tech,⋯ | $\chi^{(1)}$ |
| hometown prefecture | Tokyo, Kyoto, Okinawa,⋯ | $\chi^{(2)}$ |
| : | : | : |
| current address | Tokyo, Kyoto, Okinawa,⋯ | $\chi^{(m-1)}$ |
| age | 1,2,⋯,80,⋯ | $\chi^{(m)}$ |

Information disclosure

We define an information disclosure as a transition from $\chi^{(k)}$ to a subset of $\chi^{(k)}$. We consider that a disclosure can take place $n$ times for $\chi^{(k)}$. Accordingly, $\chi_i^{(k)}$ denotes the subset of $\chi^{(k)}$ after the $i$ th $(i \in \{0,1,\ldots,n\})$ disclosure. For example, assume that $\chi^{(1)}$ is the set of attribute values for "university". If there are two disclosures about the attribute "university", $\chi_1^{(1)}$,and $\chi_2^{(1)}$ are the subsets made by the first and second disclosures, respectively. Figure 3 shows the relationship between $\chi_1^{(1)}$ and $\chi_2^{(1)}$.

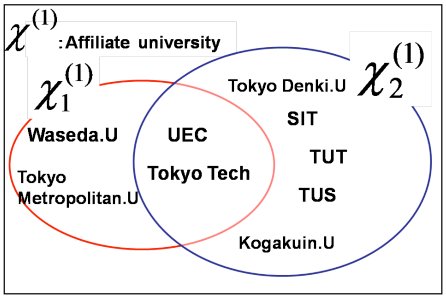


**Fig. 3. Sets of attribute values after two disclosures about attribute "university"**

Joint attribute set

$\tilde{\chi}^{(k)}$ is defined as the intersection of $\chi_1^{(k)}, \chi_2^{(k)}, \ldots, \chi_n^{(k)}$: $\tilde{\chi}^{(k)} = \bigcap_{i=1}^{n} \chi_i^{(k)}$. In figure 3, $\tilde{\chi}^{(1)}$ is $\tilde{\chi}^{(1)}$ ={UEC, Tokyo Tech}, and $\tilde{\chi}^{(k)}$ is the joint set of $n$ information disclosures.

### 5.2 Quantification of revelations

The revelation of private information is quantified in terms of the difference in entropy before and after information is disclosed. Specifically, joint entropy is used to quantify revelations about a person with multiple attributes.

#### 5.2.1 Privacy revelations of a single attribute

We start by quantifying a revelation of private information about a single attribute. We assume that information about the $k$th attribute of a person is disclosed.

First, we calculate the entropy before disclosure:

$$H(X^{(k)}) = -\sum_{x} P(X^{(k)} = \mathrm{x}) \log_2 P(X^{(k)} = \mathrm{x}) \cdots (1)$$

Next, we calculate the entropy after disclosure:

$$H(\tilde{X}^{(k)}) = -\sum_{\mathrm{x} \in X^{(1)}} P(\tilde{X}^{(k)} = \mathrm{x}) \log_2 P(\tilde{X}^{(k)} = \mathrm{x}) \cdots (2)$$

The value of the revelation for the $k$th attribute is thus

$$\Delta^{(k)} = H(X^{(k)}) - H(\tilde{X}^{(k)}) \cdots (3)$$

#### 5.2.2 Revelations of multiple attributes

The total value of all revelations for all attributes is represented by $\Delta$. That is, $\Delta$ denotes the difference in the joint entropy of $m$ attributes before and after disclosures.

$$\Delta = H(\{X^{(k)}\}) - H(\{\tilde{X}^{(k)}\}) \cdots (4)$$

The entropy before multiple disclosures is given by

$$H(\{X^{(k)}\}) = H(X^{(1)}, X^{(2)}, \ldots, X^{(k)}) \cdots (5)$$

The entropy after multiple disclosures is given by

$$H(\{\tilde{X}^{(k)}\}) = H(\tilde{X}^{(1)}, \tilde{X}^{(2)}, \ldots, \tilde{X}^{(k)}) \cdots (6)$$

To compute $H(\{X^{(k)}\})$ and $H(\{\tilde{X}^{(k)}\})$, we transform equations (7) and (8) into the conditional entropy for multiple sets of attribute values.

$$H(X^{(1)}, X^{(2)}, \ldots, X^{(k)})$$
$$= H(X^{(1)}) + H(X^{(2)} \mid X^{(1)}) + \cdots + H(X^{(m)} | X^{(m-1)}, \cdots, X^{(2)}, X^{(1)}) \cdots (7)$$
$$H(\tilde{X}^{(1)}, \tilde{X}^{(2)}, \ldots, \tilde{X}^{(k)})$$

$$= H(\widetilde{X}^{(1)}) + H(\widetilde{X}^{(2)} \mid \widetilde{X}^{(1)}) + \cdots + H(\widetilde{X}^{(m)} | \widetilde{X}^{(m-1)}, \cdots, \widetilde{X}^{(2)}, \widetilde{X}^{(1)}) \cdots (8)$$

$X^{(i)}$ can be exchanged with $X^{(j)}$ for any pair of different $i$ and $j$ ($i, j = 1, \ldots, m$) ($i \neq j$).

# 6 Application to privacy revelation from SNS and database

Here we consider two attributes for *the subject*: the university he attends and his home prefecture (hometown). In our example, the person is a university student in Tokyo.

We consider three cases:

Case 1: Privacy revealed from SNS (section 6.1).

Case 2: Privacy revealed from company database compromised by third parties (section 6.2).

Case 3: The combination of case1 and case2(section 6.3).

## 6.1 Privacy revelation from SNS

### 6.1.1 One disclosure of the affiliated university attribute

We represent the set of potential universities he is attending as $\chi^{(1)}$. Before disclosure, *the subject* might be attending any university in the set.

The probability that he is attending university $x$ is expressed as follows.

$$P(X^{(1)} = \mathrm{x}) = \frac{(\text{Number of students attending university } x)}{(\text{Number of students attending all universities})}$$

We used university student population data obtained from [15] to calculate $P(X^{(1)} = \mathrm{x})$. The entropy before disclosure was calculated using by using equation (1).

$$H(X^{(1)}) = -\sum_{x} P(X^{(1)} = \mathrm{x}) \log_2 P(X^{(1)} = \mathrm{x}) = 6.0260 .$$

There are two entries that disclose information about *the subject*'s university.

*Entry 1: Next week, I will attend the job fair in the West-6 building.*
*Entry 2: I attend a science and technology university in Tokyo.*

First, we consider these entries independently.

(I) Entry 1

$\chi_1^{(1)}$ is the subset of $\chi^{(1)}$ after entry 1 is posted. We find that there are four universities that have buildings named "West-6":

$$\chi_1^{(1)} = \{\text{UEC, Tokyo Tech, Waseda Univ., Tokyo Metropolitan Univ.}\}$$

If we consider only this disclosure, $\tilde{\chi}^{(1)} = \chi_1^{(1)}$. $P(\tilde{X}^1 = \mathrm{x})$ is the probability of the subject attending university $x$.

$$P(\tilde{X}^{(1)} = \mathrm{x}) = \frac{(\text{Number of students attending university } x(\in \tilde{X}^{(1)}))}{(\sum_{x \in X^1} \text{Number of students attending university } x)}$$

$H(\tilde{X}^{(1)})$ ,which is the entropy after disclosure, is calculated by using equation(2) :

$$H(\tilde{X}^{(1)}) = -\sum_{\mathrm{x} \in \tilde{X}^{(1)}} P(\tilde{X}^{(1)} = \mathrm{x}) \log_2 P(\tilde{X}^{(1)} = \mathrm{x}) = 1.1548 .$$

Thus, once entry 1 is posted, the revelation is quantified as by using equation (3).

$$\Delta^{(1)} = H(X^{(1)}) - H(\tilde{\chi}^{(1)}) = 4.8712$$

(II) Entry 2

$\chi_2^{(1)}$ is the subset of $\chi^{(1)}$ after entry 2 is posted. Since there are seven universities of science and technology in Tokyo,

$\chi_2^{(1)}$ = {UEC, Tokyo Tech, Tokyo Denki Univ., TUT, Kogakuin Univ., TUS, SIT}.

$H(\tilde{X}^{(1)})$ and $\Delta^{(1)}$ are calculated in a similar fashion by using equation(2) and (3).

$$H(\tilde{X}^{(1)}) = 2.6331 , \quad \Delta^{(1)} = 3.929$$

### 6.1.2 Multiple disclosures about university attribute

Now consider the case in which entries 1 and 2 are considered in combination. The intersection between $\chi_1^{(1)}$ and $\chi_1^{(2)}$ is

$$\tilde{\chi}^{(1)} = \{\text{UEC, Tokyo Tech}\}.$$

$H(\tilde{X}^{(1)})$ and $\Delta^{(1)}$ are calculated in a similar fashion by using equation(2) and (3).

$$H(\tilde{X}^{(1)}) = = 0.9950 , \Delta^{(1)} = 5.0310$$

### 6.2 Privacy revelation from database

We represent the set of potential values of "hometown" as $\chi^{(2)}$. Before the disclosure, *the subject*'s hometown can be any prefecture in the set. The probability that his hometown is prefecture $x$ is expressed as follows.

$$P(X^{(2)} = \mathrm{x}) = \frac{(\text{Population in prefecture } x)}{(\text{Population in all prefectures})} .$$

We used data from [16] to calculate $P(X^{(2)} = \mathrm{x})$. The entropy before disclosures is given by using equation (1).

$$H(X^{(2)}) = 5.0842$$

We assume that *the subject*'s hometown is leaked from a company database and that *the subject*'s hometown is in Kyoto. The set obtained from this disclosure is

$$\chi_1^{(2)}=\{\text{Kyoto}\}.$$

We consider only this disclosure; that is, $\tilde{\chi}^{(2)}= \chi_1^{(2)}$ .Because his hometown address is unique now, $H(\tilde{X}^{(2)}) = 0$.
This revelation from a company database is quantified by using equation (3).

$$\Delta^{(2)} = H(X^{(2)}) - H(\tilde{X}^{(2)}) = 5.0842$$

### 6.3 Multiple disclosures of multiple attributes

The entropy before disclosures about *the subject*'s university and hometown is given by

$$H(\{X^{(2)}\}) = H(X^{(1)}, X^{(2)}) = H(X^{(1)}) + H(X^{(2)}|X^{(1)}) \cdots (9)$$

$H(X^{(2)}|X^{(1)})$ is the conditional entropy before disclosure.

$$H(X^{(2)}|X^{(1)}) = -\sum_{\mathrm{x}_q} P(X^{(1)}= \mathrm{x}_q) \bullet \sum_{\mathrm{x}_p} \{P(X^{(2)}= \mathrm{x}_p, X^{(1)}= \mathrm{x}_q) \log P(X^{(2)}= \mathrm{x}_p \,|X^{(1)}= \mathrm{x}_p)\}$$

$P(X^{(2)} \mid X^{(1)})$ is the conditional probability of $\chi^{(2)}$ when $\chi^{(1)}$ is known.

$$\mathrm{P}(\mathrm{X}^{(2)} = \mathrm{x}_\mathrm{p} \mid \mathrm{X}^{(1)} = \mathrm{x}_\mathrm{q}) = \frac{(\text{Number of students attending university } \mathrm{x}_\mathrm{q} \text{ who came from } \mathrm{x}_\mathrm{p})}{(\text{Number of students attending university } \mathrm{x}_\mathrm{q})}$$

For each university, we can determine the number of students who came from each prefecture [17]. Thus, the entropy before disclosure is expressed by using equation (9).

$$H(\{X^{(2)}\}) = 10.1420$$

Now let us consider the case that diary entries 1, 2 are disclosed and revelation from company database.The entropy after the disclosures about the user's university and hometown is expressed by using equation (8)

$$H(\{\tilde{X}^{(2)}\}) = H(\tilde{X}^{(1)}, \tilde{X}^{(2)}) = H(\tilde{X}^{(1)}) + H(\tilde{X}^{(2)}|\tilde{X}^{(1)}) \cdots (10)$$

The conditional entropy after these disclosures is calculated as follows

$$H(\tilde{X}^{(2)}|\tilde{X}^{(1)}) = -\sum_{x_q} P(\tilde{X}^{(1)}= x_q) \bullet \sum_{x_p} \{P(\tilde{X}^{(2)}= x_p, \tilde{X}^{(1)}= x_q) \log P(\tilde{X}^{(2)}= x_p \,|\tilde{X}^{(1)}= x_p)\}$$

$$P(\tilde{X}^{(2)} = x_p|\tilde{X}^{(1)} = x_q) = \frac{(\text{Number of students in university } \chi_q \text{ who came from } \chi_p (\in X^2))}{\sum_{x \in \tilde{X}^2} (\text{Number of students in university } \chi_q \text{ who came from } \chi_p (\in \tilde{X}^2))}$$

Thus, the entropy after these disclosures is expressed by using equation (10).

$$H(\{\tilde{X}^{(2)}\}) = 0.9950$$

The total value of all the revelations is expressed by using equation (4).

$$\Delta = H(X^{(1)}, X^{(2)}) - H(\{\tilde{X}^{(1)}, \tilde{X}^{(2)}) = 9.1475$$

Table 3 lists the revelation values when disclosures about the university and hometown are independent and dependent.

**Table 3. Revelations of information about different attributes**

| The kind of the attribute and diary entries | Before the disclosure $H\{(X^{(k)})\}$ | After the disclosure $H\{(\tilde{X}^{(k)})\}$ | Privacy revelation value $\Delta$ |
|---|---|---|---|
| Affiliated university (Diary entry 1,2) | 6.0260 | 0.9950 | 5.310 |
| Hometown address (Revelation from database) | 5.0842 | 0 | 5.084 |
| Affiliated university and home town address (Diary entry 1,2 and Revelation from database) | 10.1420 | 0.9950 | 9.147 |

Thus, our metric quantifies accumulated revelations of information about multiple attributes and can cope with the case in which the attributes affect each other.

## 7 Conclusion

We have described a framework for quantifying the degree of privacy lost when there are multiple disclosures of information about different attributes of a person. We defined information disclosure as a transition from the possible values of an attribute to a subset of those values. We quantify the privacy revelation in terms of the difference in joint entropy of multiple attribute values before and after disclosures. Our metric can quantify how much private information is revealed as a result of multiple disclosures of information about multiple attributes.

Our metric has two key features: it quantifies accumulated revelations about different attributes and it can handle the case in which the attributes affect each other.

Evaluation using entries posted on a social networking service and leaks from a company database showed that it is effective—it can be used to quantify privacy revelations by various types of media.

## References

1. Agrawal, R., Srikant, R.: Privacy preserving data mining. In: Proceedings of the ACM SIGMOD Conference of Management of Data, pp. 439–450. ACM (2000)

2. Agrawal, D., Aggarwal, C.C.: On the design and quantification of privacy preserving data mining algorithms. In: Proceedings of the 20th ACM SIGACT-SIGMOD-SIGART Symposium on Principle of Database System, pp. 247–255. ACM (2001)
3. Sweeney, L.: Achieving k-Anonymity Privacy Protection Using Generalization and Suppression.: International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, p. 571-588,(2002).
4. Ashwin, M., Danier, K., Johannes, G., Muthuramakrishnan, V.:1-diversity: Privacy beyond k-anonymity. In: Proceedings of the 22nd IEEE International Conference on Date Engineering, Atlanta Georgia (2006)
5. Ninghui, L., Tiancheng, Li., Suresh, V.: t-closeness: Privacy beyond k-anonymity and ldiversity. In: Proceedings of the 23nd International Conference on Data Engineering (ICDE '07), Istanbul, Turkey, Apr. 16-20 (2007)
6. Baki, H., Marco,G.: Protecting location privacy through path confusion. In: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, pp.194-205, Athens, Greece (2005)
7. Duckham, M. and L. Kulik: Simulation of Obfuscation and Negotiation for Location Privacy, in Spatial Information Theory, International Conference, COSIT 2005, pp. 31-48, Springer, Ellicottville, NY, USA. (2005)
8. Gruteser, M. ,D. Grunwald: Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking, in First ACM/USENIX International Conference on Mobile Systems, Applications, and Services., pp31-42. ACM Press: San Francisco ( 2003,)
9. Hoh, B., et al.: Preserving Privacy in GPS Traces via Uncertainty- Aware Path Cloaking, In 14th ACM Conference on Computer and Communication Security, Alexandria (2007)
10. Hashem, T. and L. Kulik.: Safeguarding Location Privacy in Wireless Ad-Hoc Networks, In: 9th International Conference on Ubiquitous, pp372-290(2007)
11.John Krumm: "A survey of computational location privacy", Personal and Ubiquitous Computing, Volume 13, Issue 6(2008)
12.Claudia, D., Stefaan, S., Joris, C., Bart, P. : Towards measuring anonymity. In Workshop on Privacy Enhancing Technologies, LNCS 2482 (2002).
13.Andrei, S. , George, D.: Towards an Information Theoretic Metric for Anonymity, presented at Privacy Enhancing Technologies Workshop (PET) (2001).
14. Ken M, et. al.: Role Interchangeability and Verification of Electronic Voting, In: Proc. of SCIS(2006).
15.Nikkei Shingaku Navi, http://daigaku.shingakunavi.jp/p/
16. Statistical Database, Statistics Bureau, Director-General for Policy Planning (Statistical Standards) and Statistical Research and Training Institute, http://www.stat.go.jp-/english/data/index.htm
17. University profile ,http://www3.ibac.co.jp/univ1/mst/info/univinfo_50.jsp
18. Ryosuke, Y., Astushi, K., Takashi, H., Keiichi, H. : The Metric Model for Personal Information Disclosure. IN: Proceedings of Fourth International Conference on Disital Society(ICDS2010), pp.112-117 (2010).